

Remarks

The above Amendments and these Remarks are in reply to the Office Action mailed June 18, 2009.

I. Summary of Examiner's Rejections

Prior to the Office Action mailed June 18, 2009, Claims 1, 3-5, 7-14, 16-18, 20-25 and 51-55 were pending in the Application. In the Office Action, Claims 5 and 10 were rejected under 35 U.S.C. 112. Claims 1, 3-5, 7-14, 16-18, 20-25, 51-55 were rejected under 34 U.S.C. 103(a) as being unpatentable over Fisher (U.S. Publication No. 2003/0033535) in view of Fichtner (U.S. Publication No. 2003/0005297).

II. Applicant's Interview Summary

Applicant thanks Examiner Harris Wang for the courtesy of a telephone interview with Kuiran (TED) Liu (#60,039) and Karl Kenna (#45,445) on September 3, 2009, during the course of which interview the participants discussed the present application and claims, as described in detail in the Examiner's Interview Summary mailed September 11, 2009. No agreement was reached during the interview.

III. Summary of Applicant's Amendment

The present Reply amends Claims , 3, 10, 13, 16, 53, 54; cancels Claims 4-5, 17-18, 51, and adds new Claims 56-57, leaving for the Examiner's present consideration Claims 1, 3, 7-14, 16, 20-25 and 52-56.

IV. Claim Rejections under 35 U.S.C. §112

In the Office Action mailed June 18, 2009, Claims 5 and 10 were rejected under 35 U.S.C. 112 as lacking sufficient antecedent basis. Accordingly, Claims 5 and 10 have been amended as shown above. Applicant respectfully submits that the claims, as amended, comply with the requirements of 35 U.S.C. 112. Reconsideration thereof is respectfully requested.

V. Claim Rejections under 35 U.S.C. § 103(a)

In the Office Action mailed June 18, 2009, Claims 1, 3-5, 7-14, 16-18, 20-25, 51-55 were rejected under 34 U.S.C. 103(a) as being unpatentable over Fisher (U.S. Publication No. 2003/0033535) in view of Fichtner (U.S. Publication No. 2003/0005297).

Claim 1

Claim 1 has been amended to recite:

1. *(Currently Amended)* A system for single security administration comprising:
 - a first application server of a first server type, which is configured to execute transaction processes including receiving calls from clients to initiate the transaction processes, wherein the first application server includes
 - an access control list which defines user security information for use in authorizing the calls from clients, and
 - a Lightweight Directory Access Protocol (LDAP) authentication server plugin which is configured to forward the calls from clients to another application server for authorization;
 - a second application server of a second server type, which is configured to administer security for the first application server, wherein the second application server includes
 - a user profile database which includes security information for a plurality of users, including for each of the users a mapping of security credentials for that user between the first server type and the second server type, and
 - an embedded LDAP server which is configured to receive the calls from the LDAP authentication server plugin; andwherein, when a call is received from a client to initiate a transaction at the first application server, the LDAP authentication server plugin
 - identifies the user associated with the call,
 - determines that the second application server should authenticate the user,
 - initiates an LDAP session between the first application server and the second application server,
 - sends a query information to the embedded LDAP server,
 - receives from the embedded LDAP server a corresponding user information as determined by the user profile database at the second application server, and
 - creates a token reflecting the result, which is subsequently used to authenticate the client to participate in the transaction.

Fisher discloses a common authentication protocol or proxy (CAP) server which includes an authentication interface that communicates with directory service authentication backends. (Paragraph [0019]). As further disclosed at Paragraph [0023], Fisher describes that the CAP server obtains the user or user group information from an external source. However, as apparently acknowledged in the Office Action mailed June 18, 2009, Fisher does not explicitly teach that the CAP server holds an access control list.

Fichtner discloses that "a main focus of the present invention is to provide a database server with the capability of performing a Web single-sign-on to various backend HTTP servers. In order for this feature to be enabled, resource credential mapping capability is used to provide this goal. Essentially, a resource credential may be used to store a user's identity and password

for signing on a particular backend HTTP server. ... Resource ... data objects ... may allow an administrator to map a specific application's user identification and password to one or more multiple backend HTTP servers that require basic authentication sign-on credentials. ... Authentication server will be based on the location of the web resource requested to find the URAF_ResCreds associated with the user, and provide the contents of UID and AuthnData to the backend HTTP server. As a result, the authentication server signs onto backend server on behalf of the user. " (Figure 9, Paragraph [0054]).

Applicant respectfully submits that, based on the above description, in Fichtner there does not appear to be any interaction in the authentication process between the different backend HTTP servers to be signed on. It further appears that, in Fichtner, the authentication server and the database server for the Web single-sign-on feature is centralized and separate from the various backend HTTP servers.

To more clearly recite the embodiment therein, Claim 1 has been amended to recite that the authentication process involves two different application servers that a user wants to sign on, including a first application server of a first server type, which is configured to execute transaction processes including receiving calls from clients to initiate the transaction processes, and a second application server of a second server type, which is configured to administer security for the first application server.

Claim 1 has also been amended to recite that the first server includes a Lightweight Directory Access Protocol (LDAP) authentication server plugin which is configured to forward the calls from clients to another application server for authorization; and the second application server includes an embedded LDAP server which is configured to receive the calls from the LDAP authentication server plugin; wherein, when a call is received from a client to initiate a transaction at the first application server, the LDAP authentication server plugin identifies the user associated with the call; determines that the second application server should authenticate the user; initiates an LDAP session between the first application server and the second application server; sends a query information to the embedded LDAP server; receives from the embedded LDAP server a corresponding user information as determined by the user profile database at the second application server; and creates a token reflecting the result, which is subsequently used to authenticate the client to participate in the transaction.

Applicant respectfully submits that these features are neither disclosed by nor obvious in view of Fisher and/or Fichtner.

In view of the above comments, Applicant respectfully submits that Claim 1, as amended, is neither anticipated by, nor obvious in view of the cited references, when considered alone or in combination. Reconsideration thereof is respectfully requested.

Claim 13

The comments provided above with regard to Claim 13 are herein incorporated by reference. Claim 13 has been amended similarly to Claim 1 to more clearly recite the embodiments therein. Applicant respectfully submits that Claim 1, as amended, are likewise neither anticipated by, nor obvious in view of the cited references, when considered alone or in combination. Reconsideration thereof is respectfully requested.

Claims 3-5, 7-12, 14, 16-18, 20-25 and 51-55

Claims 3-5, 7-12, 14, 16-18, 20-25 and 51-55 depend from and include all of the features of Claims 1 and 13 are not addressed in detail herein. Applicant respectfully submits that these claims are allowable at least as depending from an allowable independent claim, and further in view of the amendments to the independent claims, and the comments provided above. Reconsideration thereof is respectfully requested.

VI. Additional Amendments

Claims 56-62 have been newly added by the present Reply. Applicant respectfully requests that new Claims 56-62 be included in the Application and considered therewith.

VII. Conclusion


In view of the above amendments and remarks, it is respectfully submitted that all of the claims now pending in the subject patent application should be allowable, and reconsideration thereof is respectfully requested. The Examiner is respectfully requested to telephone the undersigned if he can assist in any way in expediting issuance of a patent.

Application No.: 10/731,371
Reply to Office Action dated: June 18, 2009
Reply dated: November 18, 2009

Enclosed herewith is a Petition for Extension of Time, extending the time to respond up to and including November 18, 2009. The Commissioner is authorized to charge any underpayment or credit any overpayment to Deposit Account No. 06-1325 for any matter in connection with this response, including any fee for extension of time, which may be required.

Respectfully submitted,

Date: November 18, 2009

By: 
/Kuiran (Ted) Liu/
Kuiran (Ted) Liu
Reg. No. 60,039

Customer No.: 80548
FLIESLER MEYER LLP
650 California Street, 14th Floor
San Francisco, California 94108
Telephone: (415) 362-3800
Fax: (415) 362-2928